Fig.1

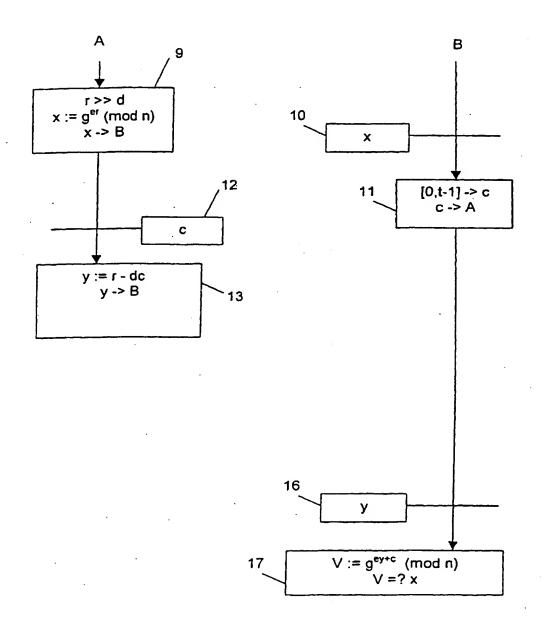
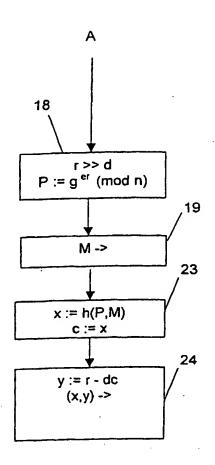
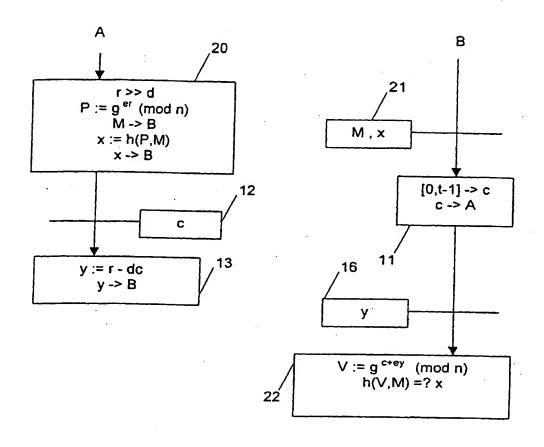


Fig.2



B c := x $V := g^{c+ey} \pmod{n}$ h(V,M) = ? x

Fig.3



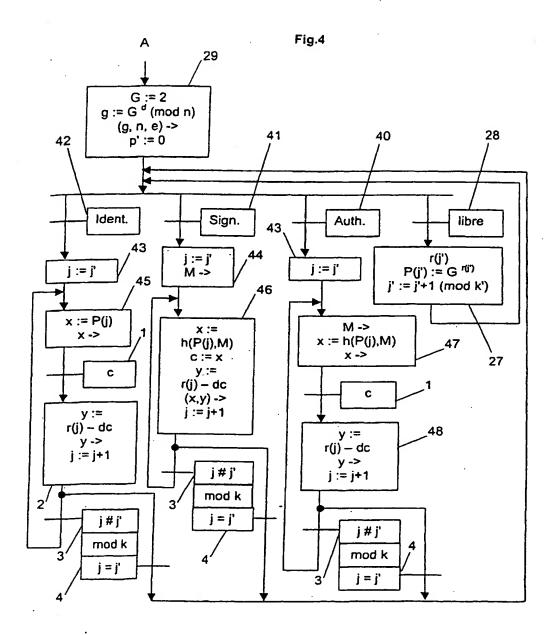


Fig.5

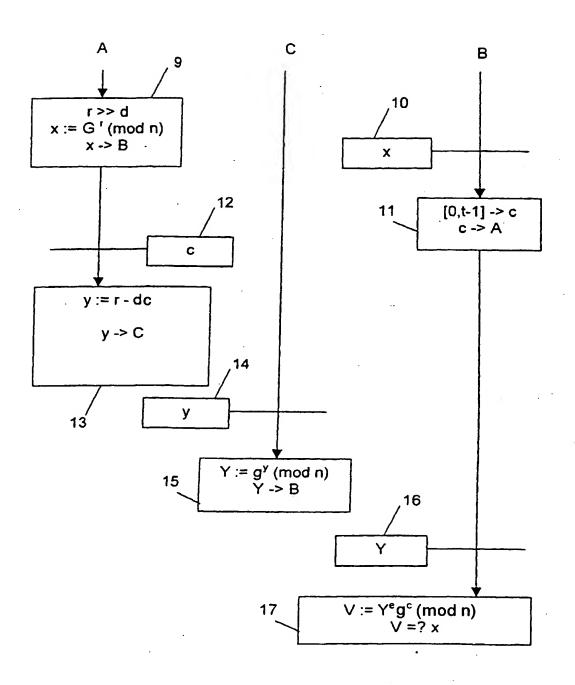


Fig.6

